ACTA ARITHMETICA
104.2 (2002)

Prime values of reducible polynomials, II

by

Yong-Gao Chen (Nanjing), Gábor Kun (Budapest),
Gábor Pete (Szeged), Imre Z. Ruzsa (Budapest) and
Ádám Timár (Szeged)

1. Introduction. It is a generally accepted conjecture that an irreducible integer-valued polynomial without a constant divisor assumes infinitely many prime values at integers. On the other hand, it is easy to see that for a reducible $f \in \mathbb{Q}[x]$ there are only finitely many integers n for which $f(n)$ is prime. It is, however, a nontrivial question to estimate the number of these integers. We shall be primarily interested in finding estimates in terms of the degree of f.

In what follows by "polynomial" we always mean a polynomial with rational coefficients, and reducibility is meant in $\mathbb{Q}[x]$. We will write

$$P(f) = \#\{m \in \mathbb{Z} : f(m) \text{ is prime}\}.$$

In the first part [3] we investigated the class of *integer-valued polynomials*, that is, such that $f(n)$ is integral whenever n is. We proved that

$$\begin{aligned}\exp\left(c\frac{n}{\log n}\right) &< \sup\{P(f) : \deg f = n, f \text{ is integer-valued and reducible in } \mathbb{Q}[x]\}\\ &< \exp\left(C\frac{n}{\log n}\right)\end{aligned}$$

with positive absolute constants c, C.

2000 *Mathematics Subject Classification*: Primary 11N32.

Research of Y. G. Chen supported by the National Natural Science Foundation of China, Grant No. 10171046 and the "333 Project" Foundation of Jiangsu Province of China. The work was done while Y. G. Chen was visiting the Mathematical Institute of the Hungarian Academy of Sciences.

Research of G. Pete supported by Hungarian National Foundation for Scientific Research, Grants No. F 026049 and T 30074.

Research of I. Z. Ruzsa supported by Hungarian National Foundation for Scientific Research, Grants No. T 025617 and T 29759.

In this part we investigate the behaviour of $P(f)$ under further restrictions. We shall assume that either

(a) the factors of f are also integer-valued, or

(b) f has integral coefficients, in which case by Gauss' lemma we may also assume that the factors have integral coefficients.

These assumptions considerably reduce the possible number of prime values. Indeed, if $f = gh$ with integer-valued g and h, then $f(x)$ can be a prime only if either $g(x) = \pm 1$ or $h(x) = \pm 1$, which immediately gives $2n$ as an upper bound. (Ore [5] attributes this observation to Stäckel [8].) Our aim is to improve this bound.

The more natural case (b) has been investigated by Ore [5]. His result sounds essentially as follows. [He formulates it indirectly (a polynomial which assumes more than... prime values must be irreducible), and does not give the construction for general n.]

THEOREM 1. *Let $f \in \mathbb{Z}[x]$ be a reducible polynomial of degree n. If $n \neq 4, 5$, then $P(f) \leq n + 2$. On the other hand, for every n there is a reducible $f \in \mathbb{Z}[x]$ such that $P(f) \geq n + 1$. If $n = 4$ or 5, then the maximal possible value of $P(f)$ is 8.*

We think that the upper bound gives the truth.

CONJECTURE 1.1. *For every n there is a reducible $f \in \mathbb{Z}[x]$ such that $P(f) = n + 2$.*

In Section 2 we outline Ore's argument, describe the construction and to support the conjecture we show that it follows from certain generally accepted but hopeless conjectures about primes.

In case (a) we can also reduce the trivial upper bound, though we are far from a complete answer.

THEOREM 2. *There is a constant $c < 2$ such that*

$$P(f) < cn + o(n)$$

for every polynomial of degree n which can be written as a product of two integer-valued nonconstant polynomials. A possible value of this constant is $c = 1.8723406362\ldots$, determined by the formula $c = 1 + 1/t$, where t is the only real root of the equation

$$t(2\log t + 1/2) = 2\log 2 - 1/2.$$

Besides $P(f)$ we will also consider

$$P^+(f) = \#\{m \in \mathbb{Z} : f(m) > 0 \text{ is prime}\}.$$

This is a less natural concept; however, the restriction to positive primes will enable us to give an exact answer. In the case considered in Part I

the discrepancy between the lower and upper bound was so large that this distinction did not matter.

THEOREM 3. *For every $n \geq 2$ and every polynomial of degree n which can be written as a product of two integer-valued nonconstant polynomials we have $P^+(f) \leq n$. On the other hand, there is a reducible $f \in \mathbb{Z}[x]$ for which $P^+(f) = n$, and consequently the maximum of P^+ in both cases* (a) *and* (b) *is exactly n.*

2. Polynomials with integer coefficients. The upper bounds stated in Theorem 1 are due to Ore [5]. We outline his argument, since the source is not easily available and also it gives some background to the construction and the related conjecture.

For a polynomial f, write

$$E^+(f) = \#\{m \in \mathbb{Z} : f(m) = 1\}, \quad E^-(f) = \#\{m \in \mathbb{Z} : f(m) = -1\},$$
$$E(f) = E^+(f) + E^-(f) = \#\{m \in \mathbb{Z} : |f(m)| = 1\}.$$

In this section by polynomial we will always mean a polynomial with integer coefficients.

The starting point is the following result of Dorwart and Ore [4].

LEMMA 2.1. *If a polynomial of degree n satisfies $E(f) > n$, then $n \leq 3$ and f is of the form $f(x) = \pm h_i(\pm x + a)$, where the polynomials h_i, $i = 1, \ldots, 5$, are listed below*:

$$\begin{aligned}
h_1(x) &= x(x-1)(x-3)+1, & n &= 3, & E(f) &= 4,\\
h_2(x) &= (x-1)(x-2)-1, & n &= 2, & E(f) &= 4,\\
h_3(x) &= 2x(x-2)+1, & n &= 2, & E(f) &= 3,\\
h_4(x) &= 2x-1, & n &= 1, & E(f) &= 2,\\
h_5(x) &= x-1, & n &= 1, & E(f) &= 2.
\end{aligned}$$

This immediately implies that if a reducible polynomial $f = gh$ satisfies $P(f) > n$, then at least one of g, h is from the above list. Furthermore, we see that $P(f) \leq n+4$, and if $P(f) = n+3$ or $n+4$, then both factors come from the list. For $n+4$ prime values, the only possibility is

$$f(x) = \pm h_2(\pm x + a)h_2(\pm x + b),$$

and indeed we get 8 prime values for

$$f(x) = (1 + x(x-3))(1 + (x-4)(x-7)).$$

For $n+3$ prime values, one of the factors must be an h_2, and the other factor has to assume prime values at four consecutive integers. However, h_3, h_4 and h_5 are easily shown not to have this property by simple divisibility

arguments. Another factor of type h_1 is possible, and an example is

$$f(x) = (1 + x(x-3))(1 + (x-4)(x-5)(x-7)).$$

This ends Ore's argument. We will now discuss the case of $n+1$ or $n+2$ prime values. The above facts show that for $n > 6$ the only possibility to have $n+2$ prime values happens when one factor is of type h_2. Thus we fix $h(x) = h_2(x)$. We show how to construct, for a given $n \geq 3$, a polynomial g of degree $n-2$ so that $f = gh$ assumes $n+2$ prime values. This construction depends on two unproved conjectures. The first is that h assumes infinitely many primes; it is a generally accepted conjecture that this holds for every irreducible polynomial without constant divisor. The next is that for every finite collection $a_1, \ldots, a_k$ of nonzero integers we can find an integer t such that all the numbers $1 + ta_i$ are prime, a version of the prime k-tuple conjecture (we will use it for $k = 4$).

Assuming the first conjecture, let $b_1, \ldots, b_{n-2}$ be distinct integers such that each $h(b_i)$ is a prime. We put

$$g(x) = 1 + t(x - b_1) \ldots (x - b_{n-2})$$

with suitable t. For every choice of t we have $f(b_i) = h(b_i) = \text{prime}$. Now the second conjecture yields the existence of a t such that $g(i)$ is prime for $i = 0, 1, 2, 3$, and then so is $f(i)$ since $h(i) = \pm 1$ for these numbers.

Ore's arguments show that this is essentially the only choice of h, hence the first conjecture is necessary.

The second conjecture can possibly be weakened for our purposes. Indeed, we do not need prime-yielding values of t for every $b_1, \ldots, b_{n-2}$; what we need is that from the set $B = \{b : h(b) \text{ is prime}\}$ we can select some $n-2$ such that the prime-quadruple conjecture works for the four numbers, determined by these $n-2$ elements of B in the above described way. Hence an average version of the prime tuple conjecture, similar to that proved by Balog [2], may suffice.

Finally we prove unconditionally that $n+1$ prime values can be attained for every $n \geq 6$. One of the factors must come from the list, and just as in the above conditional argument we need that it assume infinitely many primes. The only polynomials for which this is established are the linear ones, thus we have to use h_4 or h_5. We will use $h(x) = x = h_5(x+1)$.

Let $p_1, \ldots, p_{n-1}$ be distinct (not necessarily positive) primes. We put

$$g(x) = 1 + t(x - p_1) \ldots (x - p_{n-1})$$

with a suitable integer t. Then $f = gh$ satisfies $f(p_i) = p_i$ for $i = 1, \ldots, n-1$ and

$$f(1) = g(1) = 1 + t(1 - p_1) \ldots (1 - p_{n-1}),$$
$$f(-1) = -g(-1) = -(1 + t(-1 - p_1) \ldots (-1 - p_{n-1})).$$

In general it seems difficult to make two such expressions simultaneously prime. We get around this difficulty by selecting distinct primes $p_1, \dots, p_{n-1}$ so that

$$(1-p_1)\dots(1-p_{n-1}) = (-1-p_1)\dots(-1-p_{n-1}). \tag{2.1}$$

This will guarantee $g(-1) = g(1)$ independently of the choice of t, and if we select t to make these numbers prime, then $f(1) = g(1)$ and $f(-1) = -g(1)$ will be prime besides $f(p_i) = p_i$. This can be done by Dirichlet's theorem.

To achieve (2.1), if n is odd, we simply use primes in pairs with their negatives, that is, $p_2 = -p_1$, $p_4 = -p_3$ and so on. Every such pair contributes the same to both products.

If $n \geq 4$ is even, we use primes in pairs except the last three which will be $2, -3$ and -5. These contribute $(-1)\cdot 4\cdot 6 = (-3)\cdot 2\cdot 4 = -24$ to both sides.

Finally we mention two examples that establish the maximal value for degree 2 and 3:

$n = 2$: $f(x) = x(x-4)$: $P(f) = 4$,
$n = 3$: $f(x) = (1 + x(x-3))(x-5)$: $P(f) = 5$.

3. Integer-valued polynomials. In this section we prove Theorem 2.

LEMMA 3.1. *Let $a_1, \dots, a_k, b_1, \dots, b_k$ be $2k$ distinct integers. Write*

$$U = \prod_{i<j} |a_i - a_j|, \qquad V = \prod_{i<j} |b_i - b_j|, \qquad D = \prod_{i,j} |a_i - b_j|.$$

Then $D \geq UV(4/9)^k$.

This is Lemma 2.1 of [6].

LEMMA 3.2. *With the above notations we have*

$$D \geq (2/3)^k (1!2!\dots(2k-1)!)^{1/2}. \tag{3.1}$$

Proof. Let $c_1 < \dots < c_{2k}$ be the sequence $a_1, \dots, a_k, b_1, \dots, b_k$ arranged in increasing order. Clearly

$$W = \prod_{i<j} (c_j - c_i) \geq \prod_{1\leq i<j\leq 2k} (j-i) = 1!2!\dots(2k-1)!.$$

On the other hand, we have $W = UVD \leq D^2(9/4)^k$ by the previous lemma. (3.1) follows by comparing these inequalities. ∎

LEMMA 3.3. *Let $a_1, \dots, a_k, b_1, \dots, b_s$ be $k+s$ distinct integers, $k \leq s$. Then*

$$D = \prod_{i=1}^{k} \prod_{j=1}^{s} |a_i - b_j| \geq (2/3)^s (1!2!\dots(2k-1)!)^{s/(2k)}. \tag{3.2}$$

Proof. By the previous lemma we have

$$D = \prod_{i=1}^{k}\prod_{j=1}^{k} |a_i - b_{m_j}| \geq (2/3)^k (1!2!\dots(2k-1)!)^{1/2}$$

for every sequence $m_1, \dots, m_k$ of distinct integers satisfying $1 \leq m_j \leq s$. Multiplying these inequalities for all possible choices of the m_j and taking an appropriate root we obtain (3.2). ∎

Proof of Theorem 2. Let f be an integer-valued polynomial of degree n. We shall find an upper estimate for $E(f)$ in the form $cn + o(n)$ with the c given in the theorem.

Write $r = E^+(f)$, $s = E^-(f)$ and take integers $a_1, \dots, a_r, b_1, \dots, b_s$ so that $f(a_i) = 1$, $f(b_j) = -1$. The polynomial $F = n!f$ has integer coefficients. Write

$$F(x) + n! = A\prod_{j=1}^{n}(x - \beta_j). \tag{3.3}$$

Here A is an integer, hence $|A| \geq 1$. Since the integers b_j are roots of the polynomial $F(x)+n!$, they are listed among the β_j, say $\beta_1 = b_1, \dots, \beta_s = b_s$.

We substitute $x = a_i$ into (3.3) to obtain

$$2n! = F(a_i) + n! = A\prod_{j=1}^{n}(a_i - \beta_j). \tag{3.4}$$

For each $s + 1 \leq j \leq n$ there may be at most one i for which

$$-1/2 \leq a_i - \operatorname{Re}\beta_j < 1/2. \tag{3.5}$$

This makes altogether at most $n-s$ values of i, so there are at least $r-(n-s) = (r+s)-n$ values for which a_i does not satisfy any of the inequalities (3.5). We may assume that these are $a_1, \dots, a_k$, where $k = r + s - n$. We may also assume that $k > n/2$, since otherwise $E(f) = k + n \leq (3/2)n$ and we are ready.

Now we multiply the equations (3.4) for $i = 1, \dots, k$. This yields

$$(2n!)^k = A^k \prod_{i=1}^{k}\prod_{j=1}^{n}(a_i - \beta_j) = A^k \prod_{i=1}^{k}\prod_{j=1}^{s}(a_i - b_j)\prod_{i=1}^{k}\prod_{j=s+1}^{n}(a_i - \beta_j). \tag{3.6}$$

Observe that $k = r + s - n \leq s$.

Now we give a lower estimate for the right side of (3.6). Take first a j satisfying $s + 1 \leq j \leq n$. We have

$$|a_i - \beta_j| \geq |a_i - \operatorname{Re}\beta_j|.$$

If we arrange all the numbers $|m - \operatorname{Re}\beta_j|$, $m \in \mathbb{Z}$, in increasing order, we get the sequence $\gamma, 1-\gamma, 1+\gamma, 2-\gamma, 2+\gamma, 3-\gamma, \dots$, where γ is the distance

of $\operatorname{Re}\beta_j$ from the nearest integer. The factors of our product are k numbers from this sequence, and the first term (γ) is excluded. Since $1-\gamma \ge 1/2$, $1+\gamma \ge 1$, $2-\gamma \ge 3/2$ and so on, the product of k terms is at least

$$\frac{1}{2}\cdot\frac{2}{2}\cdot\frac{3}{2}\cdot\ldots\cdot\frac{k}{2} = \frac{k!}{2^k}.$$

In particular,

$$\prod_{i=1}^{k}|a_i-\beta_j| \ge 2^{-k}k!, \quad \prod_{i=1}^{k}\prod_{j=s+1}^{n}|a_i-\beta_j| \ge 2^{-k(n-s)}k!^{n-s}.$$

To estimate the first double product in (3.6) we use Lemma 3.3, and also $|A|^k \ge 1$. These inequalities together give

$$(2n!)^k \ge (2/3)^s(1!2!\ldots(2k-1)!)^{s/(2k)}2^{-k(n-s)}k!^{n-s}.$$

By the symmetric role of r and s we also have

$$(2n!)^k \ge (2/3)^r(1!2!\ldots(2k-1)!)^{r/(2k)}2^{-k(n-r)}k!^{n-r}.$$

We multiply these inequalities and we obtain (recall that $r+s=n+k$)

$$(2n!)^{2k} \ge (2/3)^{n+k}(1!2!\ldots(2k-1)!)^{(n+k)/(2k)}2^{-k(n-k)}k!^{n-k}.$$

To utilize this inequality we take the logarithm of both sides and use the familiar estimate

$$\log m! = m(\log m - 1) + O(\log m)$$

and the following one which can be deduced from it by an immediate calculation:

$$\log(1!2!\ldots m!) = m^2\left(\tfrac{1}{2}\log m - \tfrac{3}{4}\right) + O(m\log m).$$

We obtain

$$\begin{aligned}2kn(\log n - 1) \ge{}& k(n+k)(\log k + \log 2 - 3/2) - k(n-k)\log 2\\ &+ k(n-k)(\log k - 1) + O(n\log n).\end{aligned}$$

After dividing by k^2 and cancelling certain terms this inequality becomes

$$\frac{n}{k}\left(2\log\frac{n}{k}+\frac{1}{2}\right) \ge 2\log 2 - \frac{1}{2} + O\left(\frac{\log n}{n}\right).$$

Thus we get $n/k \ge t + o(1)$, where t is the solution of $t(2\log t + 1/2) = 2\log 2 - 1/2$. We find $t = 1.1463411865\ldots$, which leads to $r+s = k+n \le n(1+1/t)+o(n)$. The constant appearing here is $1+1/t = 1.8723406362\ldots$ ∎

Remark. Let S be an arbitrary finite set. Let $E_S(f)$ denote the number of distinct integers a such that $f(a) \in S$. The proofs of Theorems 1 and 2 depended on estimations for the value of $E_S(f)$ in the case that $S = \{-1, 1\}$. For more general finite sets S similar estimates can be obtained.

Following the approach of Dorwart and Ore, one can show that if f has integer coefficients, then $E_S(f) \le n$ except for a finite list of polynomials and their translations; in particular, $E_S(f) \le n$ for n sufficiently large. However, it seems to be a nontrivial question to find sharp estimates (in terms of the set S) for the number and maximal degree of the exceptional polynomials.

For integer-valued polynomials f we can show that $E_S(f) < Cn + o(n)$ for some absolute constant C (independent of the size of the finite set S). This can be done by modifying the proof of Theorem 2, and in this way we obtained $C = 3$.

We indicate a different proof that yields a somewhat better constant. Let K denote the maximum of absolute values of elements of S. A theorem of Pólya [6] (see also Aigner–Ziegler [1]) asserts that for a polynomial f of degree n and leading coefficient 1 the measure of real numbers satisfying $|f(x)| \le 1$ is at most 4 (in fact, the measure of the real parts of such complex numbers x is at most 4). By a natural rescaling we find that if the leading coefficient is c, then the measure of reals satisfying $|f(x)| \le K$ is at most $4(K/|c|)^{1/n}$. Since this set is the union of at most n intervals, the number of integers satisfying $|f(k)| \le K$ is at most $n + 4(K/|c|)^{1/n}$. Since for integer-valued polynomials we have $|c| \ge 1/n!$, we obtain

$$E_S(f) \le n + 4(Kn!)^{1/n} = \left(1 + \frac{4}{e}\right)n + O(\log n).$$

On the other hand, we do not have any better lower bound than $E_S(f) \ge n + 2$ for even values of n, which follows by considering

$$f(x) = a\binom{x}{k} + b$$

for suitable a, b. We cannot even achieve this for general odd n.

4. The case of positive primes. In this section we prove Theorem 3.

To show that n prime values are possible we apply the following construction. Let $p_1, \dots, p_{n-1}$ be distinct positive primes. We put $h(x) = x$ and

$$g(x) = 1 + t(x - p_1) \dots (x - p_{n-1})$$

with a suitable integer t. Then $f = gh$ satisfies $f(p_i) = p_i$ for $i = 1, \dots, n-1$ and

$$f(1) = g(1) = 1 + t(1 - p_1) \dots (1 - p_{n-1}).$$

This will be a positive prime for a suitable choice of t by Dirichlet's theorem.

Next we show that the number of prime values is at most n.

Let $f = gh$, where g, h are integer-valued polynomials of degree at least 1. If $f(m)$ is prime, then either $g(m) = \pm 1$ or $h(m) = \pm 1$. Hence the upper estimate follows from the following statement.

STATEMENT 4.1. *Let g, h be polynomials of degree at least one with real coefficients and write $f = gh$. Consider those real numbers that satisfy*

(a) $g(x) = \pm 1$ *or* $h(x) = \pm 1$, *and*
(b) $f(x) > 1$.

The total number of such reals is at most $n = \deg f$.

Proof. Let these numbers be $x_1 < \ldots < x_k$. We will show that

$$\text{(number of roots of } g') + \text{(number of roots of } h') \geq k - 2. \tag{4.1}$$

This clearly implies the statement.

We divide the points x_i into four types. Type $g+$ is defined by $g(x_i) = 1$; the types $g-$, $h+$ and $h-$ are defined analogously. By a *block* we mean a maximal sequence of consecutive x_i's of the same type; the type of the block is this type. Let l denote the number of blocks. The number of pairs x_i, x_{i+1} of equal type is then exactly $k - l$.

We call a block *extremal* if it contains x_1 or x_k, and *central* otherwise. The number of extremal blocks is 1 or 2, the number of central blocks is at least $l - 2$.

We will show that

$$\begin{aligned}\text{number of roots of } g' \geq\ &\text{(number of pairs of type } g\pm) \\ &+ \text{(number of central blocks of type } h\pm),\end{aligned} \tag{4.2}$$

and similarly

$$\begin{aligned}\text{number of roots of } h' \geq\ &\text{(number of pairs of type } h\pm) \\ &+ \text{(number of central blocks of type } g\pm).\end{aligned} \tag{4.3}$$

On adding these inequalities we get the left side of (4.1), and on the right side we have at least $(k - l) + (l - 2) = k - 2$ as claimed.

To prove (4.2) we are going to map the pairs of type $g\pm$ and blocks of type $h\pm$ onto roots of g'.

Given a pair of type $g\pm$ we have $g(x_i) = g(x_{i+1})$. Hence g' has at least one root in the interval (x_i, x_{i+1}). We map this pair to this root (or to any of such roots, if there are more than one).

Consider now a central block of type $h\pm$, say $(x_i, \ldots, x_j)$, where $1 < i \leq j < k$ by definition. For sake of definiteness assume it is of type $h+$. We have $h(x_i) = \ldots = h(x_j) = 1$, so $g(x_i) > 1, \ldots, g(x_j) > 1$. On the other hand, x_{i-1} and x_{j+1} are of a different type, and consequently $g(x_{i-1}) \leq 1$, $g(x_{j+1}) \leq 1$. We map this block onto any local maximum point of g within the interval $[x_{i-1}, x_{j+1}]$. The previous inequalities show that this cannot be any of the endpoints, thus it must be a root of g'.

We are going to show that we use any given root at most once. This has three subcases.

The roots corresponding to pairs are obviously distinct.

A root corresponding to a block is within an interval $[x_t, x_{t+1}]$, where at least one of x_t and x_{t+1} is a member of that block, in particular, it is of type $h\pm$. This shows that it cannot coincide with a root corresponding to a pair.

Consider finally two blocks, say $(x_i, \dots, x_j)$ and $(x_u, \dots, x_v)$, such that $j < u$. The corresponding roots are situated in the intervals (x_{i-1}, x_{j+1}) and (x_{u-1}, x_{v+1}), respectively. These are disjoint unless $u = j + 1$. If $u = j + 1$, then the two blocks are adjacent, hence they must be of different types, one of type $h+$ and the other of type $h-$. Hence g has a local maximum at one and a local minimum at the other, so they are distinct.

The proof of (4.3) proceeds in the same way, with the roles of g and h interchanged. ∎

Remark. Learning this result, Nándor Simányi pointed out that Statement 4.1 holds for an arbitrary ordered field. The above proof can probably be extended to this more general case; however, we can also argue as follows. For a fixed pair of degrees $(\deg g, \deg h)$ this is a first order formula in the theory of really closed ordered fields. This theory is complete, and we already know that the statement is true for $\mathbb{R}$, therefore it is true for an arbitrary really closed field. Finally, every ordered field has a really closed extension, and the validity of the statement descends to subfields.

He also asked whether a generalization of Statement 4.1 could be valid for the case of complex polynomials g, h and complex values of $x_1, \dots, x_k$. We found that the answer is "no", as shown by the following example:

$$g(z) = \tfrac{1}{3}z^3 - z + 1, \qquad h(z) = \tfrac{2}{9}(z-2)^2 + 1.$$

Here $\deg(gh) = 5$ but we have six "bad" x_i's: $g(0) = g(\pm\sqrt{3}) = h(2) = 1$, $h(2 \pm 3i) = -1$, and $gh(x_i) \in (1, \infty)$ for all of them.

This example now raises the question whether the maximal number of possible complex x_i's is equal to the trivial upper bound $2(\deg g + \deg h)$. So far we have not been able to find more than six "bad" values for the pair of degrees $(2, 3)$; a reason for this may be Bézout's theorem on the number of intersections of the real algebraic curves $g^{-1}(\mathbb{R})$ and $h^{-1}(\mathbb{R})$.

Acknowledgements. We are grateful to the referee for several corrections and for suggesting the problem of estimating $E_S(f)$ for general sets (Remark at the end of Section 3), and to John Rickard for the information on Pólya's inequality.

References

[1] M. Aigner and G. M. Ziegler, *Proofs from the Book*, Springer, 1999.

[2] A. Balog, *The prime k-tuplets conjecture on average*, in: Analytic Number Theory (Allerton Park, 1989), Birkhäuser, Boston, 1990, 47–75.

[3] Y. G. Chen and I. Z. Ruzsa, *Prime values of reducible polynomials I*, Acta Arith. 95 (2000), 185–193.

[4] H. L. Dorwart and O. Ore, *Criteria for the irreducibility of polynomials*, Ann. of Math. 34 (1933), 81–94.

[5] O. Ore, *Einige Bemerkungen über Irreduzibilität*, Jahresber. Deutsch. Math.-Verein. 44 (1934), 147–151.

[6] G. Pólya, *Beitrag zur Verallgemeinerung des Verzerrungssatzes auf mehrfach zusammenhangenden Gebieten*, Sitzungsber. Preuss. Akad. Wiss. Berlin 1928, 228–232; also in Collected Papers, Vol. 1, MIT Press, 1974, 347–351.

[7] I. Z. Ruzsa, *Large prime factors of sums*, Studia Sci. Math. Hungar. 27 (1992), 463–470.

[8] P. Stäckel, *Arithmetische Eigenschaften ganzer Funktionen*, J. f. Math. 148 (1918), 101–112.

Department of Mathematics
Nanjing Normal University
Nanjing 210097, Jiangsu, P.R. China
E-mail: ygchen@pine.njnu.edu.cn

Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged, Hungary
E-mail: gpete@sol.cc.u-szeged.hu
tadam@petra.hos.u-szeged.hu

Department of Computer Science
Eötvös University
Kecskeméti utca 10-12
H-1053 Budapest, Hungary
E-mail: kungabor@cs.elte.hu

Mathematical Institute
of the Hungarian Academy of Sciences
Pf. 127, H-1364 Budapest, Hungary
E-mail: ruzsa@math-inst.hu

Received on 7.11.2000
and in revised form on 11.12.2001 (3916)